Your Ref: 0023-0209JP
Our Ref: PA1120

**Translation of Selected Portions of Pat. Laid-open Official Gazette**

---

Appln. No: 8-258440
Appln. Date: September 30, 1996
Laid-open Pub. No: 10-107795
Laid-open Pub. Date: April 24, 1998

Inventor(s): Mariko Kondo
Applicant(s): Hitachi Software Engineering K.K.
Attorney(s): Osayoshi Akita

---

1. Title of the Invention

NETWORK MANAGEMENT SYSTEM

2. Claims

(omitted)

3. Detailed Description of the Invention (Selected Portions)

1)

(omitted)

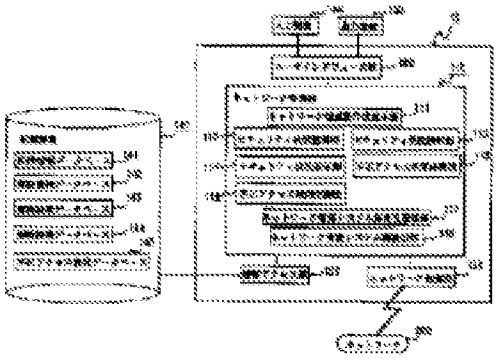
# NETWORK MANAGEMENT SYSTEM

**Publication number:** JP10107795
**Publication date:** 1998-04-24
**Inventor:** KONDOU MARIKO
**Applicant:** HITACHI SOFTWARE ENG
**Classification:**
**- international:** ***G06F13/00; H04L12/24; H04L12/26;*** **G06F13/00**; **H04L12/24**; **H04L12/26**; (IPC1-7): H04L12/24; G06F13/00; H04L12/26
**- European:**
**Application number:** JP19960258440 19960930
**Priority number(s):** JP19960258440 19960930

**Report a data error here**

Abstract of **JP10107795**

PROBLEM TO BE SOLVED: To allow the system to detect an act by the network manager to destroy the security due to mistake or on purpose by monitoring the internal security according to a specific system. SOLUTION: A security status analysis section 113 analyzes monitor result data in a monitor result database 143 stored by a security status monitor section 112 and stores the result to an analysis result database 144. In the case of this analysis, such items as time, frequency of access, device security level and qualification of access party are checked and the result of analysis is stored based on a prescribed criterion. An illegal access discrimination processing section 115 discriminates the result of analysis of the analysis result database 144 as to whether the result comes from normal access or illegal access based on the criterion of an illegal access discrimination database 145. An illegal access tendency grasp section 116 analyzes the tendency of occurrence of illegal access and executes transaction such as alarming/access reject to the external network depending on the status.



(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平10－107795

(43)公開日　平成10年(1998)４月24日

| (51)Int.Cl.[6] | | 識別記号 | Ｆ Ｉ | | |
|---|---|---|---|---|---|
| Ｈ０４Ｌ | 12/24 | | Ｈ０４Ｌ | 11/08 | |
| | 12/26 | | Ｇ０６Ｆ | 13/00 | ３５５ |
| Ｇ０６Ｆ | 13/00 | ３５５ | | | |

審査請求　未請求　請求項の数７　ＯＬ　（全 22 頁）

(21)出願番号　特願平8－258440

(22)出願日　平成８年(1996)９月30日

(71)出願人　000233055
日立ソフトウエアエンジニアリング株式会社
神奈川県横浜市中区尾上町６丁目81番地

(72)発明者　近藤　麻里子
神奈川県横浜市中区尾上町６丁目81番地
日立ソフトウェアエンジニアリング株式会社内

(74)代理人　弁理士　秋田　収喜

(54)【発明の名称】　ネットワーク管理システム

(57)【要約】

【課題】　ネットワーク管理者の立場にある者が、故意または過失によりセキュリティを破壊する行為を検出すること。

【解決手段】　ネットワーク管理システムにおいて、配置情報データベースと、監視情報データベースと、監視結果データベースと、解析結果データベースとを備え、配置データベースに格納された情報に基づき、論理的または物理的なネットワーク構成図面を表示させるネットワーク構成図作成表示手段と、監視情報データベースに基づき、ネットワークにおける内部的なセキュリティ状況を監視し、その監視結果を監視結果データベースに格納する内部的セキュリティ状況監視手段と、監視結果データベースに格納された監視結果を基に、内部的なセキュリティ状況を解析し、その解析結果を解析結果データベースに格納する内部的なセキュリティ状況解析手段と、解析結果データベースを基に、ネットワークにおける内部的なセキュリティ状況を前記ネットワーク構成図面上に表示させる内部的セキュリティ状況表示手段を備える。

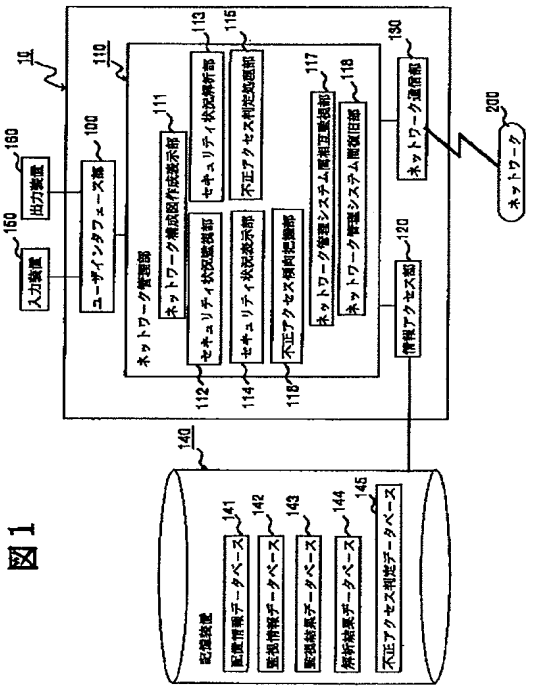



図１

1

【特許請求の範囲】

【請求項１】　電子計算機を含む複数のネットワーク機器が接続されているネットワークを管理運用するネットワーク管理システムであって、

前記ネットワーク機器の物理的配置と接続関係に関する情報を格納する第１データベースと、前記電子計算機を含む複数のネットワーク機器の監視項目及び監視内容を格納する第２データベースと、前記第２データベースの内容に従った監視結果を格納する第３データベースと、前記第３データベースに格納された監視結果を、前記ネットワーク機器毎に、時刻、頻度、使用者情報に基づいて解析した解析結果を格納する第４データベースとを備え、

前記第１データベースに格納された情報に基づき、論理的または物理的なネットワーク構成図面を表示させるネットワーク構成図作成表示手段と、

前記第２データベースに基づき、前記ネットワークにおける内部的なセキュリティ状況を監視し、その監視結果を前記第３データベースに格納する内部的セキュリティ状況監視手段と、

前記第３データベースに格納された監視結果を基に、内部的なセキュリティ状況を解析し、その解析結果を前記第４データベースに格納する内部的なセキュリティ状況解析手段と、

前記第４データベースを基に、ネットワークにおける内部的なセキュリティ状況を前記ネットワーク構成図面上に表示させる内部的セキュリティ状況表示手段を備えたことを特徴とするネットワーク管理システム。

【請求項２】　前記請求項１に記載のネットワーク管理システムにおいて、前記第４データベースに格納された解析結果に関して、各々のアクセスが正常なものであるか、不正なものによるものかを判断するための判断基準を格納する第５データベースを備え、

前記第５データベースを基に、前記ネットワーク機器に対して不正アクセスが行われたか或いは行われているかを判定して、前記内部的セキュリティ状況表示手段により表示する不正アクセス判定手段を備えたことを特徴とするネットワーク管理システム。

【請求項３】　前記請求項２に記載のネットワーク管理システムにおいて、

前記不正アクセス判定手段で不正アクセスと判定された場合に、その不正アクセスに対する対策を行う手段を備えたことを特徴とするネットワーク管理システム。

【請求項４】　前記請求項１または請求項２のいずれかに記載されたネットワーク管理システムにおいて、

前記セキュリティ状況表示手段は、そのセキュリティ状況、または不正アクセス判定における緊急度及び重要度に応じて表示形式を変えて表示する手段を備えたことを特徴とするネットワーク管理システム。

【請求項５】　前記請求項２に記載のネットワーク管理

2

システムにおいて、

前記第４データベースに格納する解析結果を一定期間蓄積し、その蓄積結果と前記第５データベースを用いて、前記ネットワーク機器に対する不正アクセスの傾向把握を行う不正アクセス傾向把握手段を備えたことを特徴とするネットワーク管理システム。

【請求項６】　前記請求項２に記載のネットワーク管理システムにおいて、

前記ネットワークが複数のサブネットワークで構成され、それらサブネットワークにそれぞれネットワーク管理システムが接続されている場合には、

各々のネットワーク管理システムが備えた前記第４データベースに格納された解析結果を相互にチェックし、あるネットワーク管理システムの管理下のサブネットワークで不正アクセスを検出した場合に、その不正アクセスが検出されたサブネットワークとのアクセスを一時中断するネットワーク管理システム間相互監視手段を備えたことを特徴とするネットワーク管理システム。

【請求項７】　前記請求項６に記載のネットワーク管理システムにおいて、

前記ネットワーク管理システム間相互監視手段により、一時的に中断しているサブネットワーク間のアクセスを不正アクセスに対する対策を行った後に復旧するネットワーク管理システム間復旧手段を備えたことを特徴とするネットワーク管理システム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、ネットワークを円滑に運用管理するためのネットワーク管理システムに関し、特に、ネットワークのセキュリティ管理を行うネットワーク管理システムに適用して有効な技術に関するものである。

【０００２】

【従来の技術】ネットワークのセキュリティ管理に関する技術では、例えば、（１）特開平０５－１０８４８７号公報の「コンピュータウィルス侵入防止装置と侵入防止方式」、（２）特開平０６－３３７７８１号公報の「情報処理装置」、（３）特開平０７－７８１７９号公報の「情報ファイル装置」、（４）特開平０７－９９４８９号公報の「パスワード制御方法および装置」、（５）特開平０７－２４８９７５号公報の「電子機器のセキュリティ保護装置」、（６）特開平０７－２６２１３５号公報の「セキュリティ管理装置」、（７）特開平０７－２６４１７８号公報の「セキュリティ方式」、などがある。

【０００３】前記（１）のコンピュータウィルス侵入防止装置と侵入防止方式は、要求がコンピュータに取り込まれた時点で、正常かウィルスによるものかをウィルスの侵入事前チェックを行い判断するものである。

【０００４】前記（２）の情報処理装置は、コンピュー

タウィルスのパターンを保存し、バッファに格納する入力データを比較し、一致した場合は、警報信号を送出し、インターフェイスを停止するものである。

【０００５】前記（３）の情報ファイル装置は、画像情報検索の利用状況を履歴情報として記録し、一定件数(警告件数)以上の検索があった場合、警告表示し、最大件数まで達すると、媒体に保存するものである。

【０００６】前記（４）のパスワード制御方法および装置は、使用装置に異常パスワードが次々入力された場合、データ保存し処理データを不定にし、２回又は５回固定パスワードを表示するものである。

【０００７】前記（５）の電子機器のセキュリティ保護装置は、セキュリティ侵害検出機構で不正アクセスを検出し、電子機器内部のデータに対するアクセスの禁止やデータ消去により、データの盗用を防止するものである。

【０００８】前記（６）のセキュリティ管理装置は、オープン型の分散ネットワーク環境でセキュリティオーディットサーバを設け、ネットワーク接続された機器からのセキュリティ侵害を検出した結果をレポート化し、その分析結果からセキュリティの弱点を診断し、セキュリティポリシーの改変要求を行うものである。

【０００９】前記（７）のセキュリティ方式は、不正アクセスがネットワーク上の端末で行われた場合に、アラーム情報とアクセス履歴情報を用いて、どのＬＡＮ上に接続された端末かを特定するものである。

【００１０】

【発明が解決しようとする課題】しかしながら、前記従来のネットワークのセキュリティ管理に関する技術は、ネットワークに不正侵入すること、または不正アクセスを行うことを防止することといった不正利用者のネットワーク利用を防止することが主な目的であったため、ネットワークを利用できる人（正規利用者）が悪用することを防止するといったことは考慮されておらず、以下に挙げるような問題点があった。

【００１１】（１）ネットワーク管理システムの管理対象であるネットワーク接続された電子計算機やネットワーク機器の正規利用者で、かつ、ネットワーク管理を行うネットワーク管理者の立場にある者が、ネットワーク管理を行う際に有する特権を用いて、故意または過失によりセキュリティを破壊する行為を行った場合に、それを検出できるものはない。

【００１２】（２）前記ネットワーク管理者が行う特権を用いたネットワーク管理作業において、正当な管理作業なのか、不正な行為なのかを判断できない。

【００１３】（３）前記ネットワーク管理者が行う特権を用いたネットワーク管理作業で不正アクセスが検出された場合に、ネットワーク上の他の電子計算機やネットワーク機器に対する安全性を確保する、即ち、セキュリティ対策を施せるものはない。

【００１４】本発明の第一の目的は、ネットワーク管理システムの管理対象であるネットワーク接続された電子計算機やネットワーク機器の正規利用者で、かつ、ネットワーク管理を行うネットワーク管理者の立場にある者が、ネットワーク管理を行う際に有する特権を用いて、故意または過失によりセキュリティを破壊する行為を行った場合に、それを検出することができるネットワーク管理システムを提供することである。

【００１５】本発明の第二の目的は、ネットワーク管理者が行う特権を用いたネットワーク管理作業において、正当な管理作業なのか、不正な行為なのかを判断できるネットワーク管理システムを提供することである。

【００１６】本発明の第三の目的は、ネットワーク管理者が行う特権を用いたネットワーク管理作業で不正アクセスが検出された場合に、ネットワーク上の他の電子計算機やネットワーク機器に対する安全性を確保する、即ち、セキュリティ対策を施せるネットワーク管理システムを提供することである。

【００１７】

【課題を解決するための手段】本願において開示される発明のうち、代表的なものの概要を簡単に説明すれば、下記のとおりである。

【００１８】電子計算機を含む複数のネットワーク機器が接続されているネットワークを管理運用するネットワーク管理システムであって、前記ネットワーク機器の物理的配置と接続関係に関する情報を格納する第１データベースと、前記電子計算機を含む複数のネットワーク機器の監視項目及び監視内容を格納する第２データベースと、前記第２データベースの内容に従った監視結果を格納する第３データベースと、前記第３データベースに格納された監視結果を、前記ネットワーク機器毎に、時刻、頻度、使用者情報に基づいて解析した解析結果を格納する第４データベースとを備え、前記第１データベースに格納された情報に基づき、論理的または物理的なネットワーク構成図面を表示させるネットワーク構成図作成表示手段と、前記第２データベースに基づき、前記ネットワークにおける内部的なセキュリティ状況を監視し、その監視結果を前記第３データベースに格納する内部的セキュリティ状況監視手段と、前記第３データベースに格納された監視結果を基に、内部的なセキュリティ状況を解析し、その解析結果を前記第４データベースに格納する内部的なセキュリティ状況解析手段と、前記第４データベースを基に、ネットワークにおける内部的なセキュリティ状況を前記ネットワーク構成図面上に表示させる内部的セキュリティ状況表示手段を備える。

【００１９】また、前記第４データベースに格納された解析結果に関して、各々のアクセスが正常なものであるか、不正なものによるものかを判断するための判断基準を格納する第５データベースを備え、前記第５データベースを基に、前記ネットワーク機器に対して不正アクセ

スが行われたか或いは行われているかを判定して、前記内部的セキュリティ状況表示手段により表示する不正アクセス判定手段を備える。

【００２０】さらに、前記ネットワークが複数のサブネットワークで構成され、それらサブネットワークにそれぞれネットワーク管理システムが接続されている場合には、各々のネットワーク管理システムが備えた前記第４データベースに格納された解析結果を相互にチェックし、あるネットワーク管理システムの管理下のサブネットワークで不正アクセスを検出した場合に、その不正アクセスが検出されたサブネットワークとのアクセスを一時中断するネットワーク管理システム間相互監視手段を備える。

【００２１】

【発明の実施の形態】以下、本発明の実施例を図面を参照して具体的に説明する。

【００２２】図１は本発明の一実施形態にかかるネットワーク管理システムの構成を説明するための機能ブロック図である。

【００２３】図１に示すように、本実施形態のネットワーク管理システム１０は、キーボード、マウスなどの入力装置１５０とディスプレイ、プリンタ、スピーカなどの出力装置１６０と接続され、データの入出力を制御するユーザインターフェイス部１００と、ネットワーク（内部ネットワーク）２００に接続された管理対象機器を管理するネットワーク管理部１１０と、ハードディスク、磁気テープ、光磁気ディスクなどの記憶装置１４０の情報をアクセスする情報アクセス部１２０と、ネットワーク２００と接続され、その通信を制御するネットワーク通信部１３０とからなる。

【００２４】上述したネットワーク管理部１１０は、図１に示すように、ネットワーク構成図を作成して表示するネットワーク構成図作成表示部１１１と、ネットワーク２００の内部的なセキュリティ状況を監視するセキュリティ状況監視部１１２と、ネットッワーク２００の内部的なセキュリティ状況を解析するセキュリティ状況解析部１１３と、ネットワーク構成図作成表示部１１１で作成表示されたネットワーク構成図面上に内部的なセキュリティ状況を表示するセキュリティ状況表示部１１４と、ネットワーク２００内部で不正アクセスが行われているか判定する不正アクセス判定部１１５と、不正アクセスに関する解析結果を蓄積し、その結果から傾向把握を行う不正アクセス傾向把握部１１６と、ネットワーク管理システム１０が相互に不正アクセスを監視し、あるネットワーク管理システムの管理下のサブネットワークで不正アクセスを検出した場合に、その不正アクセスが検出されたサブネットワークとのアクセスを一時中断するネットワーク管理システム間相互監視部１１７と、不正アクセスを検出したネットワークとの通信を復旧するネットワーク管理システム間復旧部１１８とからなる。



【００２５】また、記憶装置１４０は、図１に示すように、ネットワーク管理システム１０が管理する管理対象機器（電子計算機、ネットワーク機器、端末、ケーブル）などの物理的配置と接続関係に関する情報を格納する配置情報データベース１４１（第１データベース）と、ネットワーク管理システム１０の管理対象機器である電子計算機またはネットワーク機器に関するセキュリティ管理のための監視項目及び監視内容を格納する監視情報データベース１４２（第２データベース）と、監視情報データベース１４２に格納する監視項目と監視内容に従って、管理対象機器を監視した結果を格納する監視結果データベース１４３（第３データベース）と、監視結果データベース１４３に格納する監視結果をチェックし解析した結果を格納する解析結果データベース１４４（第４データベース）と、解析結果データベース１４４に格納された解析結果が正常なアクセスによるものか、不正なアクセスによるものかを判断するための判断基準を格納する不正アクセス判定データベース１４５（第５データベース）とからなる。

【００２６】図２は、本実施形態のネットワーク管理システム１０の管理対象である内部ネットワーク２００の全体構成を説明するための摸式的構成図である。図２において、３００はネットワーク管理システム１０の管理対象外である外部ネットワーク、３０１は外部ネットワーク３００とネットワーク管理システム１０の管理対象である内部ネットワーク２００とを接続するファイアウォール、３０２はネットワーク管理システム１０の管理対象である内部サブネットワークが複数接続する内部ネットワーク２００の基幹ネットワーク部、３０３ａ～ｃはネットワーク管理システム１０が管理する内部サブネットワークＡ，Ｂ，Ｃである。

【００２７】本実施形態における内部ネットワーク２００とは、ファイアウォール３０１の基幹ネットワーク部３０２との接続部分から、内部サブネットワークＡ３０３ａ，内部サブネットワークＢ３０３ｂ，内部サブネットワークＣ３０３ｃまでを含めたものである。

【００２８】ここで、ファイアウォール３０１は、外部ネットワーク３００と内部ネットワーク２００間の通信を制御し、内部から外部へ出ていく情報や、外部から内部に入ってくる情報の監視を行うものである。

【００２９】また、基幹ネットワーク部３０２は、通常高速ＬＡＮと呼ばれる数１０～数１００Ｍｂｐｓ程度の転送速度を有するネットワークで、各内部サブネットワーク３０３間の通信や、内部サブネットワーク３０３から外部への通信に利用される。この基幹ネットワーク部の形状は、図３のようなバス型以外に、スター型、あるいは、リング型で構成される場合もある。

【００３０】なお、内部ネットワーク２００は、ファイアウォール３０１により外部ネットワーク３００から守られており、外部ネットワーク３００からの不正侵入や

情報盗聴は発生しないものとする。また、基幹ネットワーク部３０２に複数の内部サブネットワークＡ３０３ａ，Ｂ３０３ｂ，Ｃ３０３ｃが接続した構成になっており、これら内部サブネットワークＡ３０３ａ，Ｂ３０３ｂ，Ｃ３０３ｃ間では相互通信が可能になっているものとする。

【００３１】図３は、本実施形態のネットワーク管理システム１０の管理対象となる上述した内部サブネットワーク３０３の論理的なネットワーク構成とネットワーク管理システム１０の関係を説明するための模式的構成図である。

【００３２】論理的ネットワーク構成とは、ネットワーク上で電子計算機、端末、ネットワーク機器、周辺機器がどのように接続してるかを示すものである。

【００３３】図３において、４０１は基幹ネットワーク部４００と内部サブネットワーク３０３を接続する基幹ネットワーク接続機器であり、４０２は内部サブネットワーク３０３の通信網であり、４０３は内部サブネットワーク３０３で使用するハブ等のネットワーク機器であり、４０４は端末であり、４０５は電子計算機である。

【００３４】図３に示したように、本実施形態のネットワーク管理システム１０は、基幹ネットワーク接続機器４０１を介して、基幹ネットワーク部３０２に接続する通信網４０２と、その通信網４０２に接続しているネットワーク機器４０３、端末４０４、電子計算機４０５を管理対象とする。

【００３５】また、図３に示した内部サブネットワーク３０３とは、ネットワーク管理システム１０の管理対象である通信網４０２と、ネットワーク機器４０３と、端末４０４と、電子計算機４０５と、基幹ネットワーク部３０２への接続を行う基幹ネットワーク接続機器４０１とまでを含めたものであり、各内部サブネットワーク３０３ａ～３０３ｃには、必ずその内部サブネットワーク３０３を管理する図１に示すネットワーク管理システム１０が接続されている。

【００３６】図３に示したネットワーク管理システム１０は、接続されている内部サブネットワーク３０３の通信網４０２を流れている全ての通信内容を監視（モニタリング）し、その内容を解析する。

【００３７】さらに、ネットワーク管理システム１０は、通信網４０２を介して、各々の電子計算機４０５、ネットワーク機器４０３、端末４０４の通信内容や、稼働しているプログラムやコマンド群をモニタリングし、その内容を解析する。

【００３８】これらの解析を実現するために、本実施形態のネットワーク管理システム１０は、特権モードで稼働する。特権モードとは、他の如何なるプログラムやコマンドに対しても、特権的な動作が可能な状態のことである。特権モードで稼働する場合、一般のユーザに対し書き込みを禁止しているファイルの書換えや、他のユーザが起動しているプログラムの強制停止といった動作が行える。

【００３９】また、本実施形態のネットワーク管理システム１０の特権モードでの稼動は、ネットワークや電子計算機の管理を目的としたログイン名（ユーザＩＤ）を使用する特権ユーザにより可能となる。

【００４０】また、図３に示す各内部サブネットワークＡ３０３ａ、Ｂ３０３ｂ、Ｃ３０３ｃで稼働するネットワーク管理システム１０は、相互に通信し、互いの保持する情報を交換する。

【００４１】次に、図１に示した各データベース１４１～１４５の構成について説明する。

【００４２】図４は、配置情報データベース１４１の構成を示す図である。配置情報データベース１４１には、ネットワーク管理システム１０が管理する電子計算機４０５、ネットワーク機器４０３、端末４０４、通信網（ケーブル）４０２などの物理的配置と接続関係に関する情報を格納する。図４に示すように、配置情報データベース１４１には、ネットワーク管理システム１０の管理対象機器である電子計算機４０５、ネットワーク機器４０３、端末４０４、ケーブル４０２一つ一つに対して付けられたユニークな番号である管理対象ＩＤ６０１と、後述するネットワーク構成図上の物理的位置を表す配置情報６０２と、電子計算機４０５、ネットワーク機器４０３、端末４０４、ケーブル４０２間の接続関係を表す接続情報６０３とが格納される。

【００４３】図５は、監視情報データベース１４２の構成を示す図である。監視情報データベース１４２にはネットワーク管理システム１０の管理対象機器である電子計算機４０５またはネットワーク機器４０３に関するセキュリティ管理のための監視項目及び監視内容を格納する。図５に示すように、監視情報データベース１４２には、図４の６０１と同様に、ネットワーク管理システム１０の管理対象機器である電子計算機４０５やネットワーク機器４０３に対して付けられたユニークな番号である管理対象ＩＤ７０１と、その管理対象ＩＤ７０１で示される電子計算機４０５やネットワーク機器４０３に対して、どのような項目を監視するかを示す監視項目７０２と、その監視項目７０２に対してどのような監視を行うかを示す監視内容７０３とが格納される。

【００４４】図６は、監視結果データベース１４３の構成を示す図である。監視結果データベース１４３には、図５に示した監視情報データベース１４２に格納する監視項目７０２と監視内容７０３に従って、管理対象機器を監視した結果を格納する。図６に示すように、監視結果データベース１４３には、図４の６０１及び図５の７０１と同様に、ネットワーク管理システム１０の管理対象機器である電子計算機４０５やネットワーク機器４０３に対して付けられたユニークな番号である管理対象ＩＤ８０１と、図５の７０１と同様に、管理対象機器の監

視項目８０２と、ネットワーク管理システム１０が図５の監視情報データベース１４２に格納された監視項目７０２と監視内容７０３に従って、管理対象ＩＤ８０１の電子計算機４０５やネットワーク機器４０３に対して監視した結果である監視結果８０３とが格納される。監視結果８０３は、監視項目８０２別に時系列にソートして格納される。

【００４５】図７は、解析結果データベース１４４の構成を示す図である。解析結果データベース１４４は、図６の監視結果データベース１４３に格納する監視結果８０３を以下のようなチェック項目に基づき解析した結果を解析結果として格納する。

【００４６】（１）いつ監視すべき事象が発生したか
（２）どの位の頻度で監視すべき事象が発生しているか
（３）どこで監視すべき事象が発生したか
（４）誰が監視すべき事象を発生させたか

図７に示すように、解析結果データベース１４４には、解析を行ったネットワーク管理システム１０のＩＤ９００と、監視対象である電子計算機４０５やネットワーク機器４０３の管理対象ＩＤ９０１と、図５の７０２と同様の管理対象機器に対する監視項目９０２と、その監視項目９０２に関する監視結果９０３と、その監視結果９０３に対して、上述したチェック項目の解析による解析結果９０４とが格納される。

【００４７】図８は、不正アクセス判定データベース１４５の構成を示す図である。不正アクセス判定データベース１４５は、図７の解析結果データベース１４３に格納する解決結果９０４正常なアクセスによるものか不正なアクセスによるものかを判断するための判断基準を格納する。図８に示すように、不正アクセス判定データベース１４５には、図５の７０２と同様の管理対象に対する監視項目１００１と、判断条件１００２と、監視項目１００１の解析結果９０４が判断条件１００２に合致した場合の判定結果を表す判定１００３と、監視項目１００１に関する不正アクセスが行われたときの緊急度１００４と、監視項目１００１に関する不正アクセスが行われたときの重要度度１００５と、判定１００３で不正と判定した場合の対策１００６とが格納される。

【００４８】次に、上述したネットワーク管理部１１０の各部１１２～１１８の処理について説明する。

【００４９】まず、ネットワーク管理システム１０が管理対象である電子計算機４０５やネットワーク機器４０３に対して行う内部的なセキュリティ状況の動的監視を行うセキュリティ状況監視部１１２のセキュリティ状況監視処理について図９に示したフローチャートを用いて説明する。

【００５０】セキュリティ状況監視処理は、まず、入力装置１５０から内部的なセキュリティ状況の動的監視を行うネットワーク名をネットワーク管理システム１０のユーザにより入力を受け（ステップ１１００）、ネットワーク構成図作成表示部１１１により出力装置１６０に、ステップ１１００で入力されたネットワーク名のネットワークのネットワーク構成図を表示する（ステップ１１０１）。

【００５１】このネットワーク構成図とは、管理対象機器とそれらの接続をそれぞれの物理的な配置図と共に表示して示すものであり、その表示例として、図１０に示すようなものが挙げられる。

【００５２】この図１０のネットワーク構成図では、図３に示した通信網４０２と、ネットワーク機器４０３と、端末４０４と、電子計算機４０５とがオフィス等のフロア図と共に表示してある。

【００５３】次に、ステップ１１０１で表示したネットワーク内に含まれる管理対象機器に関する情報を、図４の配置情報データベース１４１から検索し（ステップ１１０２）、その検索した管理対象機器に関する情報を用いて、図５の監視情報データベース１４２から管理対象機器の監視内容を検索する（ステップ１１０３）。

【００５４】その後、ステップ１１０３において検索した監視内容に従った管理対象機器での監視が行われているかをネットワーク通信部１３０にて確認し（ステップ１１０４）、その確認の結果を判断する（ステップ１１０５）。

【００５５】管理対象機器において、内部的なセキュリティ状況を監視中でなかった場合は、ステップ１１０６へ進み、監視中であった場合は、ステップ１１０７へ進む。

【００５６】ステップ１１０６では、ネットワーク管理システム１０が管理対象機器において監視を開始させる。監視を開始させると、ネットワーク管理システムは、監視結果を図６の監視結果データベース１４３に監視項目別に時系列にソートして格納する。これは、ネットワーク管理システム１０のユーザが監視中断の指示をするまでは監視が継続される。

【００５７】ステップ１１０７では、ネットワーク管理システム１０のユーザからの監視中断の指示があった場合、監視を終了する。

【００５８】このように、ネットワーク管理システム１０では、常時、図９に示すような内部的なセキュリティ状況の動的監視を行っている。

【００５９】次に、ネットワーク２００の内部的なセキュリティ状況を解析するセキュリティ状況解析部１１３のセキュリティ状況監視処理について図１１に示したフローチャートを用いて説明する。

【００６０】セキュリティ状況解析処理は、まず、内部的なセキュリティ状況の動的監視を行っている管理対象機器に関する監視結果が格納された図６の監視結果データベース１４３を検索し、管理対象機器が存在するかをチェックする（ステップ１２００）。管理対象機器が存在する間は、ステップ１２０１へ進み、存在しなくなる

と処理を終了する。

【００６１】ステップ１２００で管理対象機器が存在する場合、図６の監視結果データベース１４３を検索し、管理対象機器の監視項目８０２別の監視結果８０３が存在するかをチェックする（ステップ１２０１）。　監視項目８０２が存在する間は、ステップ１２０３へ進み、存在しなくなると、監視結果データベース１４３から次の管理対象機器を検索し、ステップ１２００に戻る（ステップ１２０２）。

【００６２】ステップ１２０１で管理対象機器の監視項目８０２が存在する場合、管理対象機器の監視項目８０２別の監視結果８０３が存在するかをチェックする（ステップ１２０３）。監視結果８０３が存在しなくなると、監視結果データベース１４３から次の監視項目８０２を検索し、ステップ１２０１に戻る（ステップ１２０５）。

【００６３】ステップ１２０３で管理対象機器の監視結果８０３が存在する場合、以下のようなチェック項目に基づき監視結果８０３を解析し、監視すべき各事象に関する解析結果を、解析を行ったネットワーク管理システムの管理と共に、図７の解析結果データベース１４４に格納する（ステップ１２０４）。

【００６４】（１）いつ監視すべき事象が発生したか
（２）どの位の頻度で監視すべき事象が発生しているか
（３）どこで監視すべき事象が発生したか
（４）誰が監視すべき事象を発生させたか
ここに示したチェック項目を具体的に説明すると、
（１）は、就業時間内か、時間外か、特に、深夜や早朝かどうかどうかの解析を行う。（２）は、同一の操作を複数回行い何等かのエラーを発生させていないか、毎日決まった時刻に特定のプロセスが起動されていないか、等の解析を行う。（３）は、アクセス権を有する管理対象機器に対するアクセスか、一般のアクセス許諾設定のされている端末かどうか、等の解析を行う。（４）は管理者かどうか、特定のプロジェクトの構成員か、一般ユーザかどうかの解析を行う。

【００６５】そして、ステップ１２０４において、監視結果８０３の解析が終了すると、ステップ１２０６に進み、監視結果データベース１４３から次の監視結果８０３を検索し、ステップ１２０３に戻る。

【００６６】このように、ネットワーク管理システム１０は、常時、図１１に示した監視結果８０３の解析を行っている。

【００６７】次に、ネットワーク構成図面上に緊急度及び重要度に応じてネットワーク２００の内部的なセキュリティ状況を表示するセキュリティ状況表示部１１４のセキュリティ状況表示処理について図１２と図１３を用いて説明する。

【００６８】セキュリティ状況表示部処理は、図１２に示すように、まず、内部的なセキュリティ状況を表示するネットワーク名を入力装置１５０からユーザにより入力を受け（ステップ１３００）、ステップ１３００で入力されたネットワーク名のネットワークのネットワーク構成図（図１０参照）を出力装置１６０に表示する（ステップ１３０１）。

【００６９】次に、ステップ１３０１で表示したネットワーク内でセキュリティ状況の動的監視と監視結果の解析を行っている管理対象機器が格納された図７の解析結果データベース１４４を検索し、管理対象機器の解析結果９０４が存在するかをチェックする（ステップ１３０２）。解析結果９０４が存在する間は、ステップ１３０３へ進み、存在しなくなると処理を終了する。

【００７０】ステップ１３０２で管理対象機器の解析結果９０４が存在する場合、不正アクセス判定条件を格納した図８の不正アクセス判定データベース１４５を検索し、図７の解析結果データベース１４４に格納した解析結果９０４との比較を行い、不正かどうかの判定を行う（ステップ１３０３）。

【００７１】不正の場合はステップ１３０５へ進み、正常の場合はステップ１３０４において、解決結果データベース１４４から次の解析結果９０４を検索し、ステップ１３０２に戻る。

【００７２】ステップ１３０３で管理対象機器の監視項目に関する解析結果９０４が不正であった場合、ステップ１３０５において、図８の不正アクセス判定データベース１４５に格納している緊急度１００４と重要度１００５に関して以下のレベルに従い、ステップ１３０１で表示したネットワーク構成図上に解析結果と不正アクセス判定結果を内部的なセキュリティ状況として表示する。

【００７３】（１）緊急度に関して：
A）即時：表示色変更・表示サイズ変更・点滅表示
B）緊急：表示色変更・表示サイズ変更
C）一般：表示色変更
（２）重要度に関して：
A）最重要：表示色変更・表示サイズ変更・点滅表示
B）重要：表示色変更・表示サイズ変更
C）一般：表示色変更
D）注意：ウォーニング表示
この緊急度を具体的に説明すると、例えば、管理対象機器のシステム自体の変更を伴うものはA）の即時、ファイルの急激な膨張によるディスク・フルを生じさせるものはB）の重要、上述のA）とB）以外の不正アクセスはC）の一般となる。

【００７４】また、重要度を具体的に説明すると、例えば、管理対象機器のシステム関連ファイルに関するものはA）の最重要、管理者のみがアクセス許諾されているものはB）重要、一般ユーザがアクセスできるものはC）の一般、誰にでもアクセスを許諾しているものはD）の注意となる。

【００７５】次に、上述した解析結果の具体的な表示例について説明する。図１３は、ネットワーク構成図面上の内部的なセキュリティ状況の表示例を示す図である。図１３において、１４００は通信網、１４０１はネットワーク機器、１４０２は電子計算機、１４０３は端末、１４０４は緊急レベルのセキュリティ状況にある被管理機器、１４０５は最重要レベルのセキュリティ状況にある被管理機器である。このように解析結果の表示を行う。

【００７６】なお、ここで述べたネットワーク管理システムがネットワーク構成図面上に緊急度及び重要度に応じた表示による内部的なセキュリティ状況の表示処理は、図１２で説明した解析処理の結果だけではなく、後述の図１５に示す不正アクセスの傾向把握処理の結果、図１７に示すネットワーク管理システムの相互監視処理の結果についても、同様に表示可能である。

【００７７】次に、ネットワーク２００において不正アクセスが行われたか或は行われているかを判定する不正アクセス判定処理部１１５の不正アクセス判定処理について図１４のフローチャートを用いて説明する。

【００７８】不正アクセス判定処理は、図１４に示すように、まず、内部的なセキュリティ状況の動的監視を行っている管理対象機器に関する解析結果が格納された図７の解析結果データベース１４４を検索し、管理対象機器の解析結果９０４が存在するかをチェックする（ステップ１５００）。解析結果９０４が存在する間は、ステップ１５０１へ進み、存在しなくなると処理を終了する。

【００７９】ステップ１５００で管理対象機器の解析結果が存在する場合、不正アクセス判定条件を格納した図１０の不正アクセス判定データベース１４５を検索し、図７の解析結果データベース１４４に格納した監視項目９０２に関する解析結果９０４と比較を行い、不正かどうかの判定を行う（ステップ１５０１）。

【００８０】不正の場合はステップ１５０３へ進み、正常の場合はステップ１５０２において、解析結果データベース１４４の解析結果９０４を検索し、ステップ１５００に戻る。

【００８１】ステップ１５０１で管理対象機器の監視項目９０２に関する解析結果が不正であった場合、図１０の不正アクセス判定データベース１４５の不正アクセスに対する対策１００６が存在するとき、その処理を行う（ステップ１５０３）。

【００８２】ステップ１５０３で不正アクセスへの対策処理が終了するとステップ１５０２に進み、図７の解析結果データベース１４４から次の解析結果を検索し、ステップ１５００に戻る。

【００８３】次に、ネットワーク管理システム１０が監視結果を一定期間蓄積し、その蓄積結果から不正アクセスの傾向把握を行う不正アクセス傾向把握部１１６における不正アクセス傾向把握処理について図１５のフローチャートを用いて説明する。

【００８４】不正アクセス傾向把握処理は、図１５に示すように、まず、入力装置１５０から内部的なセキュリティ状況の動的監視を行うネットワーク名をネットワーク管理システム１０のユーザにより入力を受け（ステップ１６００）、ネットワーク構成図作成表示部１１１により出力装置１６０に、ステップ１１００で入力されたネットワーク名のネットワークのネットワーク構成図を表示する（ステップ１６０１）。

【００８５】次に、ステップ１６０１で表示したネットワーク内でセキュリティ状況の動的監視と監視結果の解析を行っている管理対象機器に関する解析結果を格納した図７の解析結果データベース１４４を検索し、管理対象機器の解析結果９０４が存在するかをチェックする（ステップ１６０２）。解析結果９０４が存在する間は、ステップ１６０３へ進み、存在しなくなると処理を終了する。

【００８６】ステップ１６０２で管理対象機器の解析結果９０４が存在する場合、不正アクセス条件が格納された図１０の不正アクセス判定データベース１４５を検索し、図７の解析結果データベース１４４の監視項目９０２に関する解析結果９０４と比較を行い、不正かどうかの判定を行う（ステップ１６０３）。

【００８７】不正の場合はステップ１６０５へ進み、正常の場合はステップ１６０４において、解析結果データベース１４４から次の解析結果９０４を検索し、ステップ１６０２に戻る。

【００８８】ステップ１６０３で管理対象機器の監視項目９０２に関する解析結果９０４が不正だった場合、不正アクセスの傾向把握を行う（ステップ１６０５）。

【００８９】この不正アクセスの傾向把握は、不正アクセスが行われる状況を掴むためのものであり一定期間中に発生した各事象を時系列に解析し、時間的、場所的な分布を算出する。これにより、不正アクセスの時間的、場所的の傾向を把握できる。

【００９０】ステップ１６０５で不正アクセスの傾向把握が終了すると、ステップ１６０４に進み、図７の解析結果データベースの次の解析結果９０４を検索し、ステップ１６０２に戻る。

【００９１】次に、複数のネットワーク管理システム１０が稼働している場合に、各々のネットワーク管理システム１０が相互に監視結果をチェックするネットワーク管理システム間相互監視部１１７におけるネットワーク管理システム間相互監視処理について説明する。

【００９２】内部サブネットワーク３０３で稼働する複数のネットワーク管理システム１０は各々、図３に示したような内部サブネットワーク３０３の管理に加えて、基幹ネットワーク３０２に接続されている他の内部サブネットワーク３０３において、セキュリティが確保され

ているかを、ネットワーク管理システム間相互監視部１１７において特権モードを用いて監視する。

【００９３】そのネットワーク管理システム間相互監視処理は、他の内部サブネットワーク３０３で稼働しているネットワーク管理システム１０が行っているセキュリティ状況の動的監視結果を用いて、他の内部サブネットワーク３０３でセキュリティが確保されているかどうかを相互に監視し合う処理である。

【００９４】もし、不正なアクセスが他の内部サブネットワーク３０３で検出された場合は、その内部サブネットワーク３０３自体を信頼できないものと判断し、その内部サブネットワーク３０３に接続されているネットワーク機器４０３、端末４０４、電子計算機４０５からのアクセス要求を一時的に拒絶する。

【００９５】これにより、不正アクセスの検出された内部サブネットワーク３０３は、他の内部サブネットワークとの通信が行えなくなり、内部ネットワーク３０３から孤立することになる。本来、ネットワーク接続は、情報や資源の共有、情報交換の高速化等を目的として行われるものであるため、内部ネットワーク２００での孤立は、内部サブネットワーク３０３内のユーザにとって、内部ネットワーク２００内で情報や資源の共有が行えず、高速な情報交換が行えなくなるという不利益が生じることになる。

【００９６】さらに、ネットワーク管理システム１０は不正アクセスを検出した他の内部サブネットワーク３０３内のユーザ全員に対し、その内部サブネットワーク３０３内で不正アクセスが行われている、即ち、セキュリティが確保されていないことを通知する。また、ある内部サブネットワーク３０３内のユーザが、不正アクセスを検出した他の内部サブネットワーク３０３に対してアクセス要求を行った場合も、そのユーザに対して、アクセス要求を行った他の内部サブネットワーク３０３は、セキュリティが確保されていないことを警告し、そのアクセス要求により、内部サブネットワーク３０３が危険に晒される可能性があることを通知する。

【００９７】したがって、この仕組みを内部ネットワーク２００全体で運用すると、ある内部サブネットワークにおいて、その内部サブネットワーク３０３内の特権を有する管理者が、その特権を用いて何らかの不正アクセスを行った場合に、その事実が内部ネットワーク２００全体、更に、その内部ネットワーク２００内の全ユーザに対して、公になる。

【００９８】これにより、こうした不利益を内部サブネットワーク３０３内のユーザに対して被らせるような行為を、その内部サブネットワーク３０３の管理者が行ったことが公表されることが予め自明となるため、特権を有する管理者に対して、そうした不正行為を抑制させることが可能である。

【００９９】ネットワーク管理者とはネットワーク接続による利益を得るために、環境設定等を行う立場にいる人間であるため、自らの不正行為により不利益が生じると判っている事項を、あえて行うことはなくなる。

【０１００】また、ネットワーク管理者が属する内部サブネットワーク３０３の全ユーザに、不正行為を通知されるため、ネットワーク管理者としての特権が剥奪される可能性が高くなる。つまり、自らの有している特権を失うことに繋がる行為を、故意にすることは考え難くなる。ネットワーク管理者における不正行為を防止できる。

【０１０１】さらに、ネットワーク管理システム１０がそうした不正行為をその内部サブネットワーク３０３のユーザや、他の内部サブネットワーク３０３に対して公表することは、複数の内部サブネットワーク３０３の管理者間で、相互に信頼すべき管理者かどうかを監視することになるため、管理者間で協調して不正を行うことも困難である。

【０１０２】また、相互監視による内部サブネットワーク３０３の管理ではなく、各内部サブネットワーク３０３を統括するような、内部ネットワーク２００の管理者、或は、内部ネットワーク２００にネットワーク管理システムを置いて内部ネットワーク２００全体を管理する場合は、その全体の管理者、即ち、最も強い権限を有する管理者の不正行為を検出することが非常に難しい。したがって、上位概念のネットワーク管理システムを用いて内部ネットワーク２００を管理するのと比較して、相互監視による内部サブネットワーク３０３の管理は、安全性が高いと言える。

【０１０３】次に、上述したネットワーク管理システム間相互監視処理と監視結果をチェックする処理について、図１６のフローチャートを用いて説明する。

【０１０４】ネットワーク管理システム間相互監視処理は、図１６に示すように、まず、内部的なセキュリティ状況の動的監視を行っているネットワーク管理システム１０を通信可能な他の内部サブネットワーク３０３のネットワーク管理システム１０のネットワーク通信部１３０から検索する（ステップ１７００）。

【０１０５】通信可能な他の内部サブネットワーク３０３上で稼働しているネットワーク管理システム１０があれば、ステップ１７０１へ進み、存在しなければ処理を終了する。

【０１０６】ステップ１７００で通信可能な他の内部サブネットワーク３０３上にネットワーク管理システム１０がある場合、そのネットワーク管理システム１０の解析結果が格納された図７の解析結果データベース１４４を検索し、管理対象機器の監視項目９０２別の解析結果９０４が存在するかをチェックする（ステップ１７０１）。監視項目９０２が存在する間は、ステップ１７０３へ進み、存在しなくなるとステップ１７０２において、通信可能な次のネットワーク管理システム１０を検

索し、ステップ１７００に戻る。

【０１０７】ステップ１７０１で他の内部サブネットワーク３０３上で稼働するネットワーク管理システム１０の管理対象機器の解析結果９０４が存在する場合、解析結果９０４を用いて図８の不正アクセス判定データベース１４５を検索し、現在検索しているネットワーク管理システム１０が稼働している内部サブネットワーク３０３以外の他の内部サブネットワーク３０３に通知すべき事象、すなわち不正アクセスが管理対象機器で発生していないかどうかをチェックする（ステップ１７０３）。もし、不正がある場合にはステップ１７０４へ進み、存在しなくなるとステップ１７０５において、図７の解析結果データベース１４４から次の解析結果９０４を検索し、ステップ１７０１に戻る。

【０１０８】ステップ１７０３で管理対象機器の監視項目９０２に関する解析結果９０４が不正だった場合、内部サブネットワーク３０３上で稼働する全てのネットワーク管理システム１０に対して、その内部サブネットワーク３０３内で何らかの不正アクセスを検出した旨、通知を行う。通知を受けた他のネットワーク管理システム１０は、再度、通知元のネットワーク管理システム１０から安全確認後の通知があるまで、通知元のネットワークとの通信を行わない（ステップ１７０４）。

【０１０９】不正アクセスを検出した内部サブネットワーク３０３との通信の一時的中断は、通信内容に含まれる発信元アドレスをチェックすることで行う。つまり、発信元アドレスが不正アクセスが検出された内部サブネットワーク３０３のアドレスだった場合は、その通信内容を受け取らない、無視することになる。

【０１１０】ステップ１７０４において、複数のネットワーク管理システム１０間での相互監視が終了すると、ステップ１７０６に進み、図７の解析結果データベース１４４から次の解析結果９０４を検索し、ステップ１７０３に戻る。

【０１１１】次に、上述の図１６で説明したネットワーク管理システム１０が内部サブネットワーク３０３を相互に監視する処理と監視結果をチェックする処理において、ある内部サブネットワーク３０３で不正アクセスを検出した場合に、通信不能だった内部サブネットワーク３０３が通信可能になる、即ち、不正アクセスに対する対策を実施した後、ネットワークに復旧するネットワーク管理システム間復旧部１１８のネットワーク管理システム間復旧処理について、図１７のフローチャートを用いて説明する。

【０１１２】ネットワーク管理システム間復旧処理は、図１７に示すように、まず、一定期間待つ（ステップ１８００）。

【０１１３】次に、再度不正アクセスがあった内部サブネットワーク３０３で稼働しているネットワーク管理システム１０の監視結果９０２及び解析結果９０３を再チェックする（ステップ１８０１）。

【０１１４】ステップ１８０１で再チェックした内容に不正と判断すべき事象が含まれていない場合は１８０３へ進み、含まれている場合は通信を中断したままで、ステップ１８００に戻る（ステップ１８０２）。したがって、ステップ１８０１の再チェックで不正が含まれなくなるまでは、不正アクセスがあった内部サブネットワーク３０３は、他の内部サブネットワーク３０３とは通信できない状態が続く。

【０１１５】その後、不正アクセスがあった内部サブネットワーク３０３の再チェック結果を、他の内部サブネットワーク３０３で稼働しているネットワーク管理システム１０に通知する（ステップ１８０３）。

【０１１６】通知を受けとった他の内部サブネットワーク３０３のネットワーク管理システム１０は、各々自身の判断基準で不正アクセスがあった内部サブネットワーク３０３で稼働しているネットワーク管理システム１０の監視結果及び解析結果を再チェックし、通知を行ったネットワーク管理システム１０と同様の結果が得られた場合は、通知を行ったネットワーク管理システム１０に対し、再開承認通知を送付する。

【０１１７】その後、ネットワーク管理システム１０は他の全ての内部サブネットワーク３０３で稼働しているネットワーク管理システム１０から再開承認通知が届いたかをチェックし、全てのネットワーク管理システム１０が承認した場合はステップ１８０６へ、まだ承認通知を送付していないネットワーク管理システム１０がある場合は、ステップ１８０５へ進む。

【０１１８】ステップ１８０５で一定期間待ち、全てのネットワーク管理システム１０から再開承認通知が届くまで、ステップ１８０４のチェックを繰り返す。

【０１１９】そして、全てのネットワーク管理システム１０から再開承認通知が届いた時点で、通知を行ったネットワーク管理システム１０は、通信を再開することを不正アクセスがあった内部サブネットワーク３０３を含めた、他の全てのネットワーク管理システム１０に通知する。

【０１２０】最後に、上述の図１６で説明したネットワーク管理システム間相互監視処理において、複数のネットワーク管理システム１０の相互監視結果が食い違った場合の処理について説明する。

【０１２１】複数のネットワーク管理システム１０が複数の内部サブネットワーク３０３上で稼働しているということは、常時どこかのネットワーク管理システム１０が、他の内部サブネットワーク３０３を監視していることを意味する。したがって、ある内部サブネットワーク３０３上のネットワーク管理システム１０が他の内部サブネットワーク３０３での不正アクセスを検出した場合に、別の内部サブネットワーク３０３上のネットワーク管理システム１０は、異なる監視結果、即ち、不正アク

セスを検出しないことも考えられる。また、他の内部サブネットワーク３０３のネットワーク管理システム１０の監視結果自体に不正があり、正常な解析や判断を行えない場合も想定される。

【０１２２】こうした場合に、本実施形態のネットワーク管理システム１０は、以下の方法で不正を検出した内部サブネットワーク１０に対する処理を行う。

【０１２３】まず、複数のネットワーク管理システム１０は、図５の監視情報データベース１４２に監視項目７０２及び監視内容７０３を、図６の監視結果データベース１４３に監視結果８０３を、図７の解析結果データベース１４４に解析結果９０４を、図８の不正アクセス判定データベース１４５に不正アクセスの判断基準１００２を、各々内部で保有している。なお、不正アクセス判定データベース１４５に格納する不正アクセスの判断基準１００２は、内部ネットワーク２００内で共通である。

【０１２４】したがって、あるネットワーク管理システム１０が、他の内部サブネットワーク３０３の監視を行った時点での解析結果９０４が、別のネットワーク管理システム１０の解析結果９０４と異なる場合は、最新の解析結果９０４を有するネットワーク管理システム１０を信頼する。

【０１２５】但し、ある内部サブネットワーク３０３の管理者が特権を用いて、ネットワーク管理システム１０自体に改竄を行い、不正の検出を正常に行っていない場合は、最新の解析結果９０４であっても信頼することはできない。

【０１２６】そこで、異なる解析結果９０４を有する、他の内部サブネットワーク３０３のネットワーク管理システム１０があった場合、ネットワーク管理システム１０は、異なる解析結果９０４のネットワーク管理システム１０の有する図５の監視情報データベース１４２と、図７の解析結果データベース１４４の内容を、その他の内部サブネットワーク３０３で稼働するネットワーク管理システム１０の有する各々の監視情報データベース１４３及び解析結果データベース１４４と比較する。

【０１２７】不正の検出結果及び解析結果９０４は、この監視情報データベース１４２及び解析結果データベース１４４に格納する情報によって異なるため、個々のネットワーク管理システム１０間で差異がなければ、信頼できるものと判断する。

【０１２８】また、全てのネットワーク管理システム１０が各々全く異なる解析結果９０４を有する場合は、どの内部サブネットワーク３０３も信頼できないことになり、結果的に、内部サブネットワーク３０３間の通信は、全く行われないことになる。

【０１２９】このような状況は、上述したようにネットワーク管理者はネットワーク接続のメリットを失う状況になることから考え難い。

【０１３０】したがって、多くのネットワーク管理システム１０は、同一の解析結果９０４を導き出すと考えられ、結果として、最も同じ解析結果９０４となるネットワーク管理システム１０が互いに信頼できることになる。

【０１３１】以上、説明したように、電子計算機を含む複数のネットワーク機器が接続されているネットワークを管理運用するネットワーク管理システムであって、前記ネットワーク機器の物理的配置と接続関係に関する情報を格納する配置情報データベースと、前記電子計算機を含む複数のネットワーク機器の監視項目及び監視内容を格納する監視情報データベースと、前記監視情報データベースの内容に従った監視結果を格納する監視結果データベースと、前記監視結果データベースに格納された監視結果を、前記ネットワーク機器毎に、時刻、頻度、使用者情報に基づいて解析した解析結果を格納する監視結果データベースとを備え、前記配置情報データベースに格納された情報に基づき、論理的または物理的なネットワーク構成図面を表示させるネットワーク構成図作成表示手段と、前記監視情報データベースに基づき、前記ネットワークにおける内部的なセキュリティ状況を監視し、その監視結果を前記監視結果データベースに格納する内部的セキュリティ状況監視手段と、前記監視結果データベースに格納された監視結果を基に、内部的なセキュリティ状況を解析し、その解析結果を前記解析結果データベースに格納する内部的なセキュリティ状況解析手段と、前記解析結果データベースを基に、ネットワークにおける内部的なセキュリティ状況を前記ネットワーク構成図面上に表示させる内部的セキュリティ状況表示手段を備えることにより、ネットワーク管理システムの管理対象であるネットワーク接続された電子計算機やネットワーク機器の正規の利用者で、かつ、ネットワーク管理を行うネットワーク理管者の立場にある者が、ネットワーク管理を行う際に有する特権を用いて、故意または過失によりセキュリティを破壊する行為を行った場合に、それを検出することができる。

【０１３２】また、前記解析結果データベースに格納された解析結果に関して、各々のアクセスが正常なものであるか、不正なものによるものかを判断するための判断基準を格納する不正アクセス判定データベースを備え、前記不正アクセス判定データベースを基に、前記ネットワーク機器に対して不正アクセスが行われたか或いは行われているかを判定して、前記内部的セキュリティ状況表示手段により表示する不正アクセス判定手段を備えることにより、ネットワーク管理者が行う特権を用いたネットワーク管理作業において、正当な管理作業なのか、不正な行為なのかを判断できる。

【０１３３】さらに、前記ネットワークが複数のサブネットワークで構成され、それらサブネットワークにそれぞれネットワーク管理システムが接続されている場合に

は、各々のネットワーク管理システムが備えた前記解析結果データベースに格納された解析結果を相互にチェックし、あるネットワーク管理システムの管理下のサブネットワークで不正アクセスを検出した場合に、その不正アクセスが検出されたサブネットワークとのアクセスを一時中断するネットワーク管理システム間相互監視手段を備えることにより、ネットワーク管理者が行う特権を用いたネットワーク管理作業で不正アクセスが検出された場合に、ネットワーク上の他の電子計算機やネットワーク機器に対する安全性を確保する、即ち、セキュリティ対策を施すことができる。

【０１３４】なお、上述したネットワーク管理システム１０のネットワーク管理部１１０は、コンピュータで実行可能なプログラムで実現される場合もあり、そのときのプログラムは、フロッピーディスク、ＣＤ・ＲＯＭ、マスクＲＯＭ等の記憶媒体で一般ユーザに提供される。この場合、さらに、これら処理の他にＧＵＩプログラム等の他のプログラムと組み合わせてユーザに提供することもある。

【０１３５】また、上述した記憶媒体で提供する代替手段として、インタネット等のネットワークを通じて有償で提供することもある。

【０１３６】以上、本発明者によってなされた発明を、前記実施形態に基づき具体的に説明したが、本発明は、前記実施形態に限定されるものではなく、その要旨を逸脱しない範囲において種々変更可能であることは勿論である。

【０１３７】

【発明の効果】本願において開示される発明のうち代表的なものによって得られる効果を簡単に説明すれば、下記のとおりである。

【０１３８】ネットワーク管理システムの管理対象であるネットワーク接続された電子計算機やネットワーク機器の正規の利用者で、かつ、ネットワーク管理を行うネットワーク理管者の立場にある者が、ネットワーク管理を行う際に有する特権を用いて、故意または過失によりセキュリティを破壊する行為を行った場合に、それを検出することができる。

【０１３９】また、ネットワーク管理者が行う特権を用いたネットワーク管理作業において、正当な管理作業なのか、不正な行為なのかを判断できる。

【０１４０】さらに、ネットワーク管理者が行う特権を用いたネットワーク管理作業で不正アクセスが検出された場合に、ネットワーク上の他の電子計算機やネットワーク機器に対する安全性を確保する、即ち、セキュリティ対策を施すことができる。

【図面の簡単な説明】

【図１】本発明の実施形態にかかるネットワーク管理システムのシステム構成を示す図である。

【図２】本実施形態のネットワークの全体構成を説明するための摸式的構成図である。

【図３】本実施形態のネットワーク管理システムの管理対象となる内部サブネットの論理的なネットワーク構成を説明するための図である。

【図４】配置情報データベースの構成を示す図である。

【図５】監視情報データベースの構成を示す図である。

【図６】監視結果データベースの構成を示す図である。

【図７】解析結果データベースの構成を示す図である。

【図８】不正アクセス判定データベースの構成を示す図である。

【図９】セキュリティ状況監視処理を説明するフローチャートである。

【図１０】ネットワーク構成図面の表示例を示す図である。

【図１１】セキュリティ状況解析処理を説明するフローチャートである。

【図１２】セキュリティ状況表示処理を説明するフローチャートである。

【図１３】セキュリティ状況の表示例を示した図である。

【図１４】不正アクセス判定処理を説明するフローチャートである。

【図１５】不正アクセス傾向把握処理を説明するフローチャートである。

【図１６】ネットワーク管理システム間相互監視処理を説明するフローチャートである。

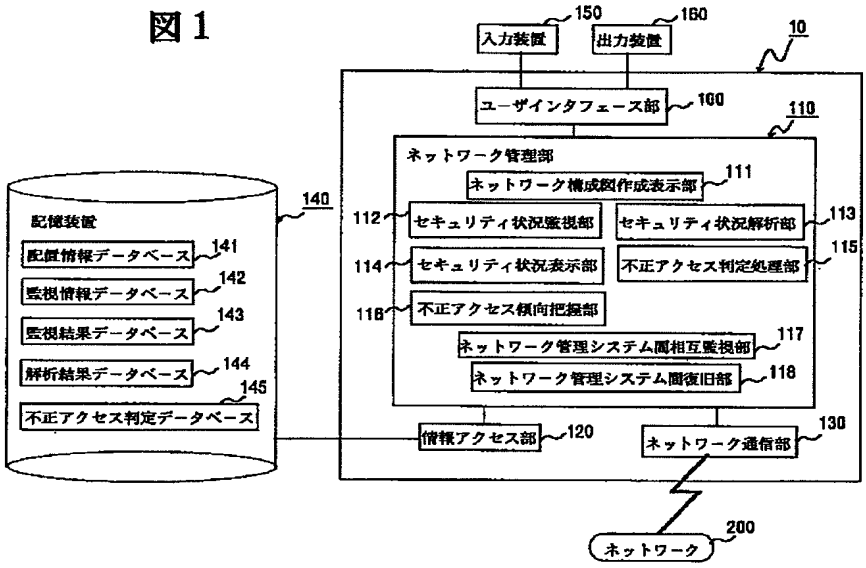
【図１７】ネットワーク管理システム間復旧処理を説明するフローチャートである。

【符号の説明】

１０…ネットワーク管理システム、１００…ユーザインターフェイス部、１１０…ネットワーク管理部、１１１…ネットワーク構成図作成表示部、１１２…セキュリティ状況監視部、１１３…セキュリティ状況解析部、１１４…セキュリティ状況表示部、１１５…不正アクセス判定部、１１６…不正アクセス傾向把握部、１１７…ネットワーク管理システム間相互監視部、１１８…ネットワーク管理システム間復旧部、１２０…情報アクセス部、１３０…ネットワーク通信部、１４０…記憶装置、１４１…配置情報データベース（第１データベース）、１４２…監視情報データベース（第２データベース）、１４３…監視結果データベース（第３データベース）、１４４…解析結果データベース（第４データベース）、１４５…不正アクセス判定データベース（第５データベース）、１５０…入力装置、１６０…出力装置、２００…ネットワーク。

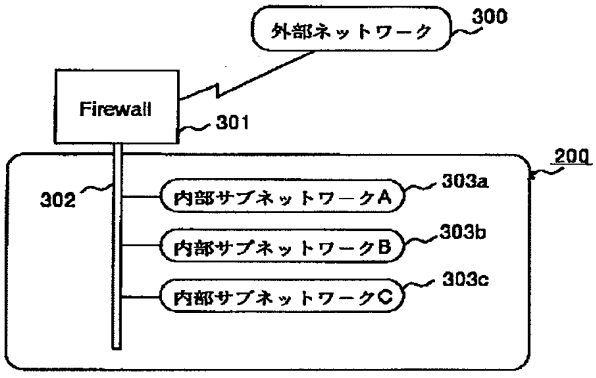
【図１】

図１



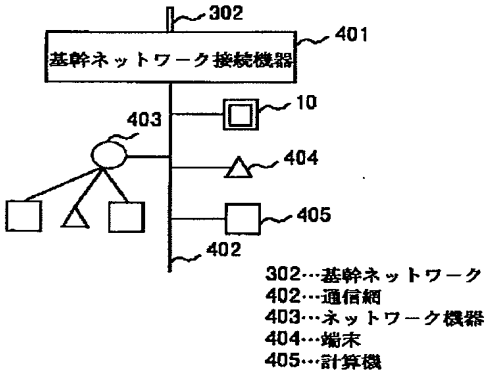

【図２】

図2




【図３】

図3




【図５】

図５

| 701 管理対象ＩＤ | 702 監視項目 | 703 監視内容 |
|---|---|---|
| １１０２１ | ログイン | 常時ログ取得 |
| ２６３５９ | 特権プロセス | SUID チェック／週 |
| ： | ： | ： |

142

【図４】

# 図４

601 602 603

| 管理対象ＩＤ | 配置情報 | 接続先ＩＤ |
|---|---|---|
| １１０２１ | 東京本社ビル/3F/x=20:y=45 | ２４８２０ |
| ２６３５９ | 東京本社ビル/8F/x=58:y=12 | ６２０ |
| : | : | : |

１４１

【図６】

# 図６

801 802 803

| 管理対象ＩＤ | 監視項目 | 監視結果 |
|---|---|---|
| ５１１０２１ | ログイン | 1995/11/24 03:21:54 JST login from A to B (user C) |
| | | 1995/11/24 05:04:11 JST login from D to A (user E) |
| | : | : |
| １２６３５９ | 特権プロセス | 1995/11/24 00:15:37 JST su from I to F (user H) |
| | | 1995/11/24 04:40:53 JST SUID proc X running at Y |
| | : | : |
| : | : | : |

１４３

【図７】

図 7

| 900 管理ＩＤ | 901 対象ＩＤ | 902 監視項目 | 903 監視結果 | 904 解析結果 |
|---|---|---|---|---|
| 523452 | 656252 | ログイン | 1995/11/24 03:19:09 SU edit file A | 就業時間外アクセス |
| 523452 | 12353 | 特権プロセス | 1995/11/24 03:21:54 SUID proc M | 一般ユーザの特権プロセス起動 |
| : | : | : | : | : |

144

【図８】

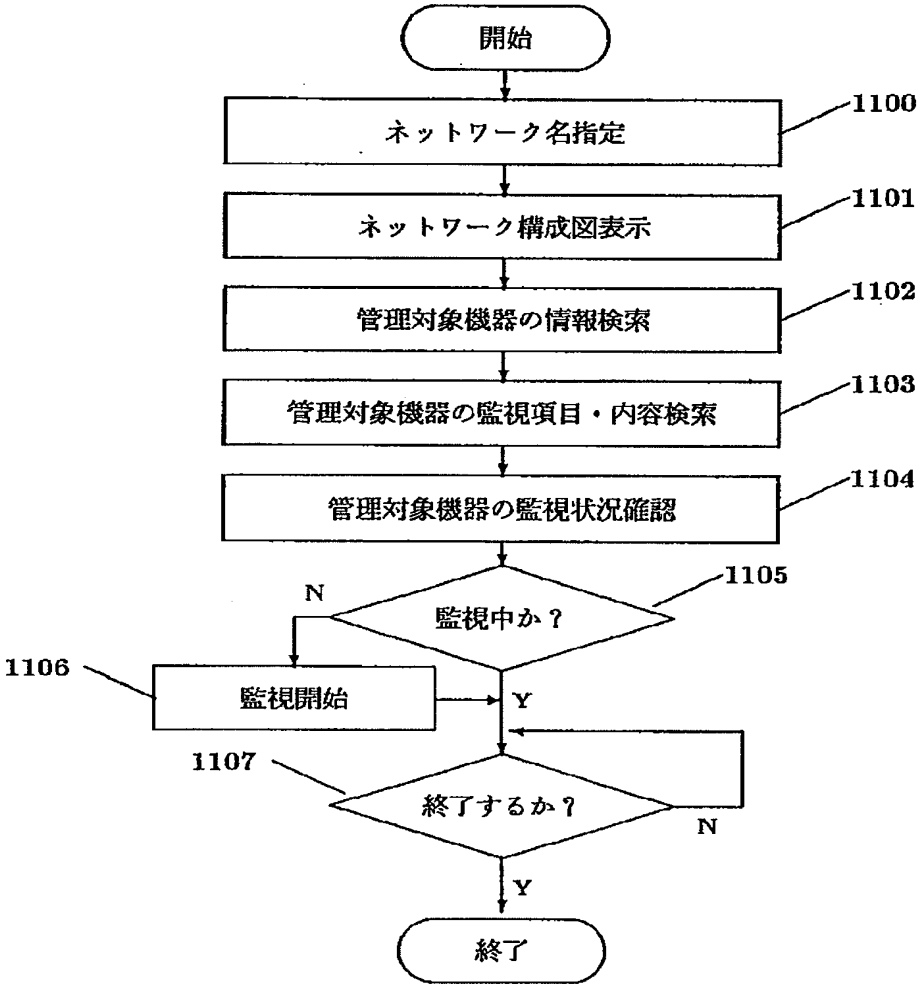
図 8

| 1001 監視項目 | 1002 判断条件 | 1003 判定 | 1004 緊急度 | 1005 重要度 | 1006 対策 |
|---|---|---|---|---|---|
| ログイン | 就業時間外アクセス | 不正 | 一般 | 重要 | 追跡調査 |
| | 就業時間内アクセス | 正常 | — | — | — |
| 特権プロセス | システム管理用ファイル更新 | 不正 | 緊急 | 最重要 | 強制終了 |
| : | : | : | : | : | : |

145

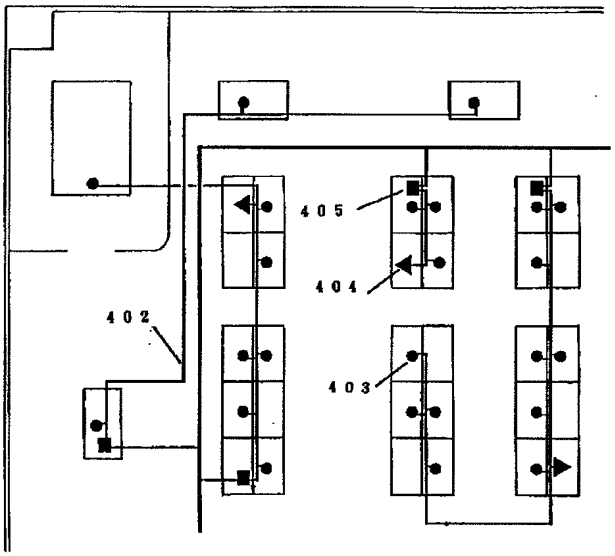
【図９】

# 図９


開始
ネットワーク名指定
1100
ネットワーク構成図表示
1101
管理対象機器の情報検索
1102
管理対象機器の監視項目・内容検索
1103
管理対象機器の監視状況確認
1104
監視中か？
1105
N
Y
監視開始
1106
終了するか？
1107
N
Y
終了

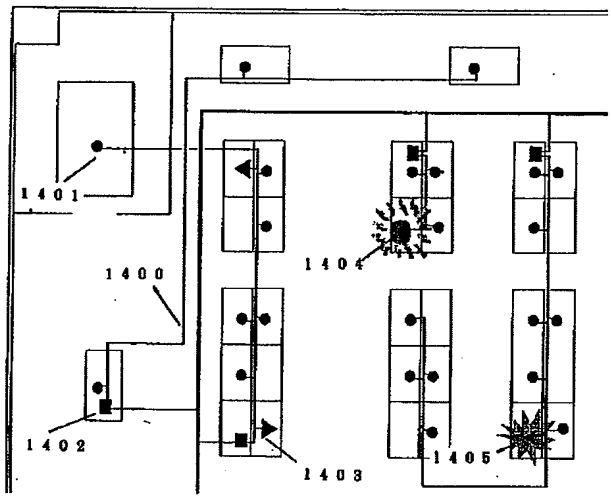
【図１０】

図１０



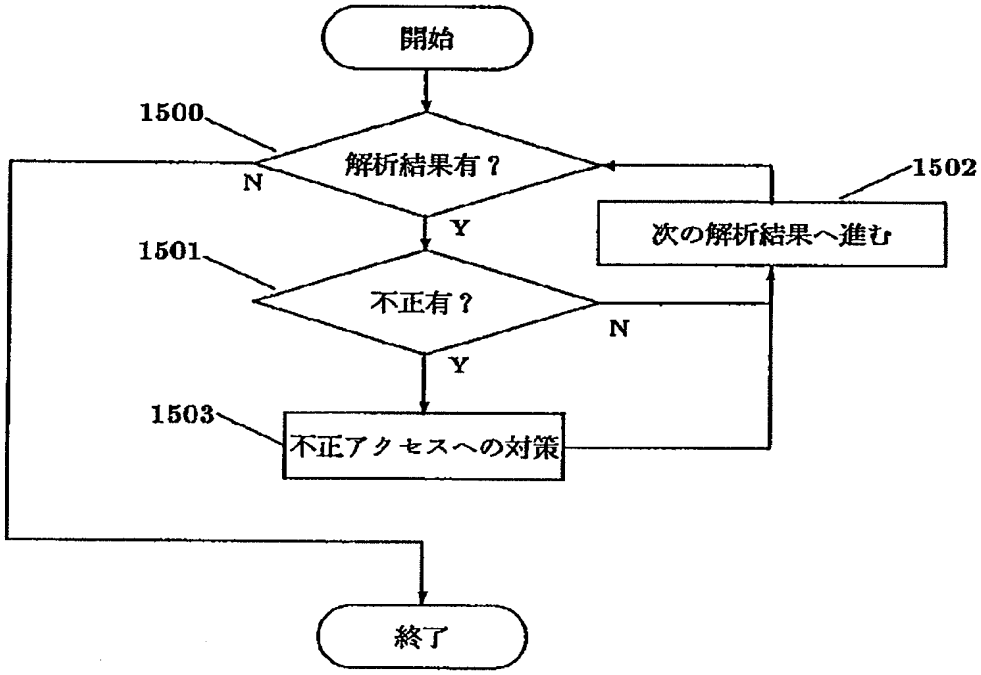

【図１３】

図１３



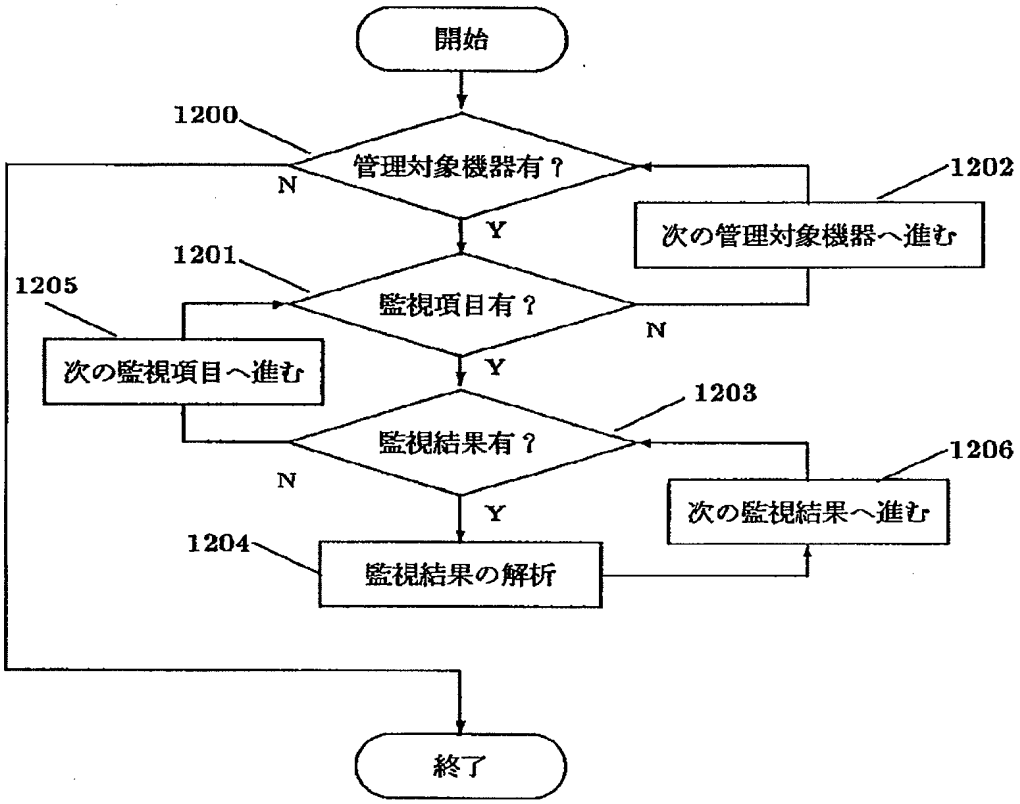

【図１４】

図１４



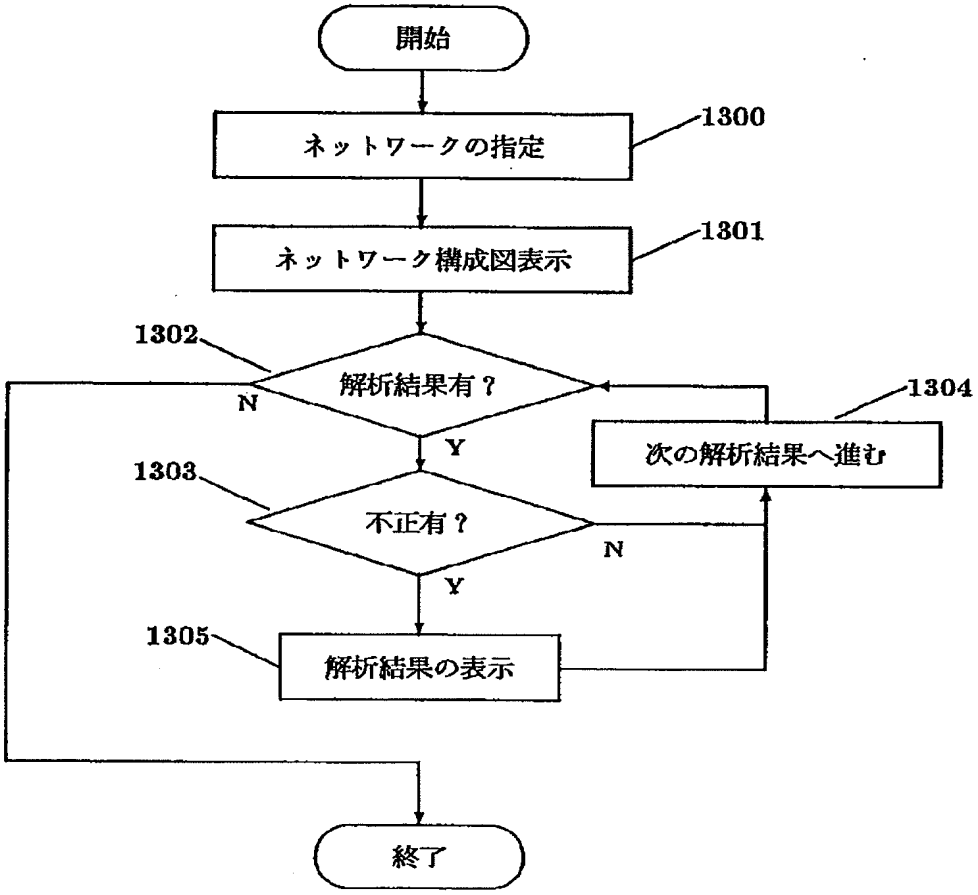
【図１１】

# 図１１


開始
1200
管理対象機器有？
N
Y
1202
次の管理対象機器へ進む
1201
監視項目有？
N
Y
1205
次の監視項目へ進む
1203
監視結果有？
N
Y
1206
次の監視結果へ進む
1204
監視結果の解析
終了

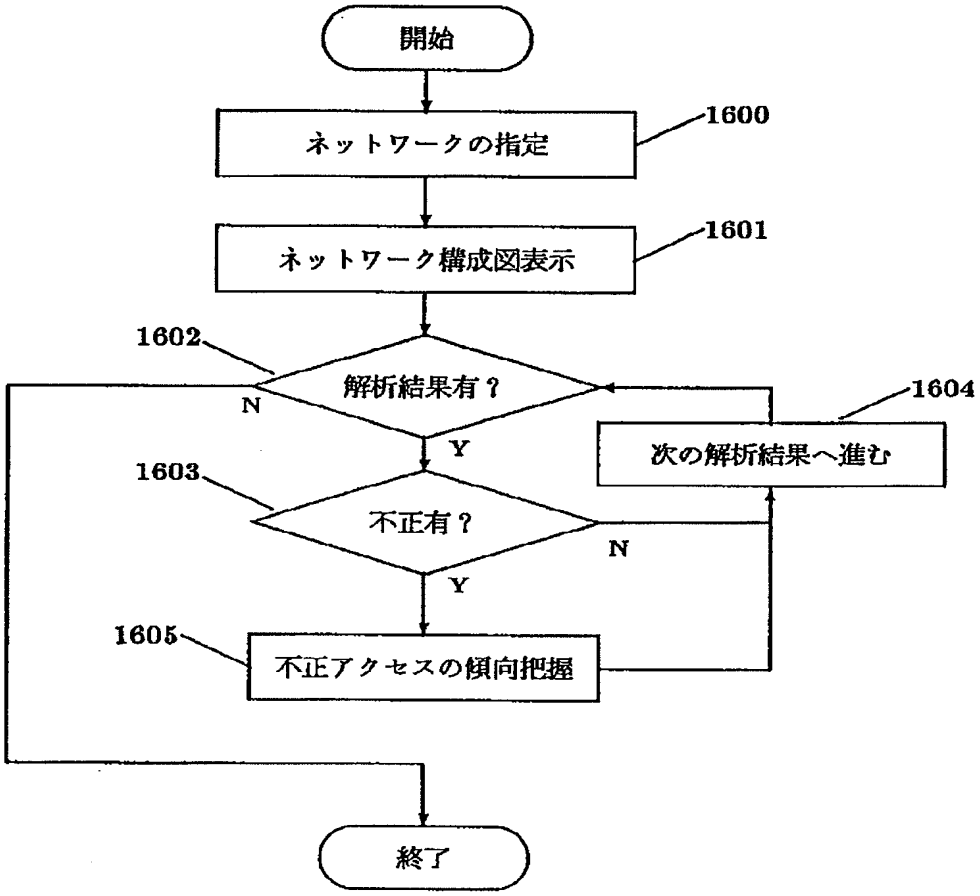
【図１２】

図１２


開始
ネットワークの指定
1300
ネットワーク構成図表示
1301
1302
解析結果有？
N
Y
1304
次の解析結果へ進む
1303
不正有？
N
Y
1305
解析結果の表示
終了

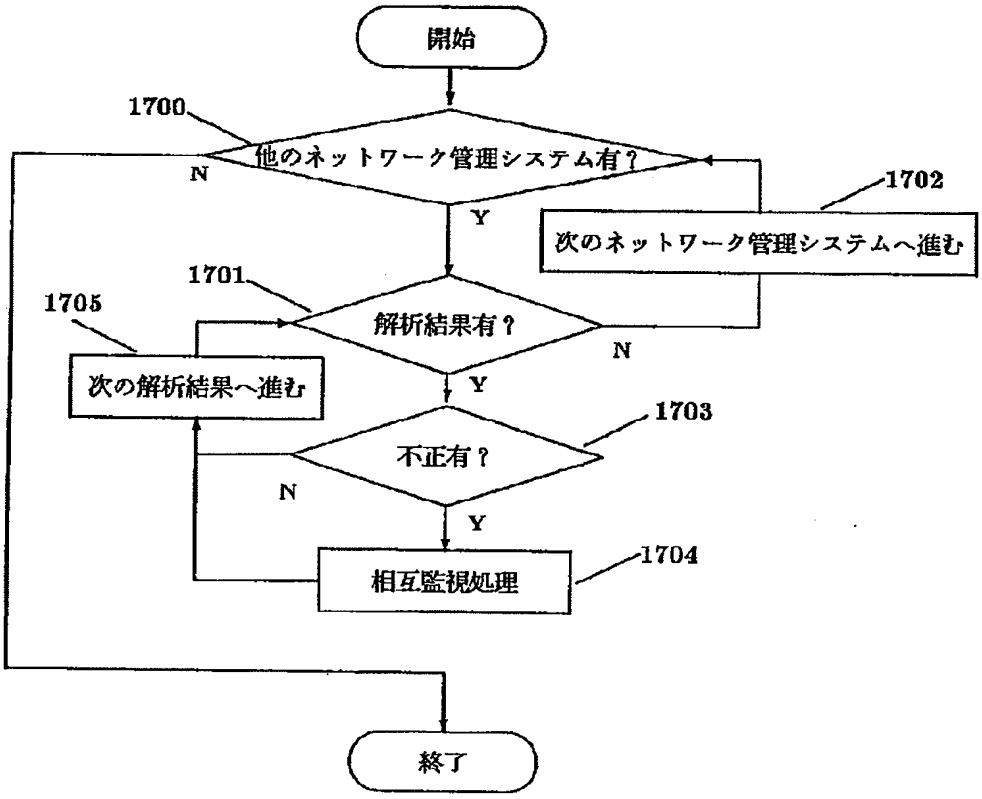
【図１５】

# 図１５


開始
ネットワークの指定
1600
ネットワーク構成図表示
1601
1602
解析結果有？
N
Y
1604
次の解析結果へ進む
1603
不正有？
N
Y
1605
不正アクセスの傾向把握
終了

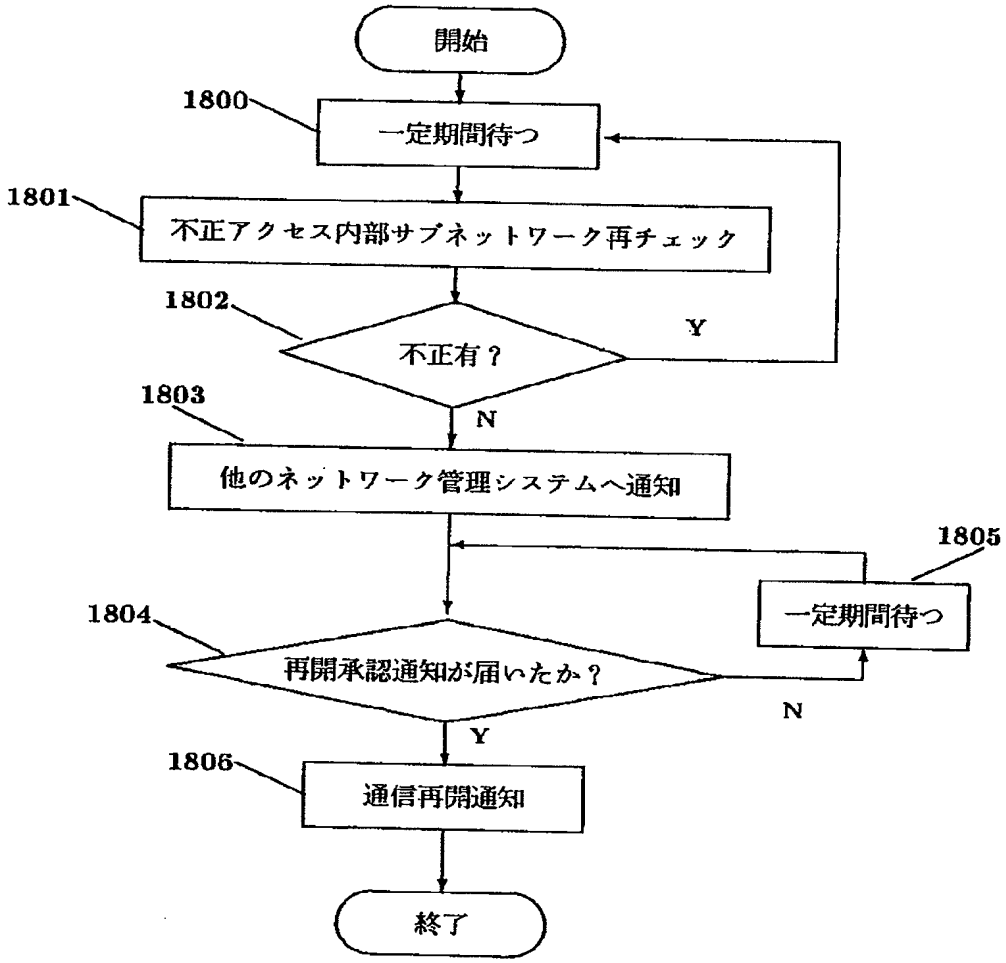
【図１６】

# 図１６


開始
1700
他のネットワーク管理システム有？
N
Y
1702
次のネットワーク管理システムへ進む
1701
解析結果有？
N
Y
1705
次の解析結果へ進む
1703
不正有？
N
Y
1704
相互監視処理
終了

【図１７】

# 図１７


開始
1800
一定期間待つ
1801
不正アクセス内部サブネットワーク再チェック
1802
不正有？
Y
N
1803
他のネットワーク管理システムへ通知
1805
一定期間待つ
1804
再開承認通知が届いたか？
N
Y
1806
通信再開通知
終了